IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

K.MIZRA LLC, Plaintiff, v. GOOGLE LLC, Defendant.	Civil Action No.: 1:25-cv-00236-ADA Jury Trial Demanded

PLAINTIFF K.MIZRA LLC'S RESPONSE IN OPPOSITION TO DEFENDANT GOOGLE LLC'S MOTION TO DISMISS UNDER FEDERAL RULE OF CIVIL PROCEDURE 12(b)(6) (ECF NO. 25)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

I. INTRODUCTION

Google LLC ("Google") offers to its worldwide business customers a product sold under the name Chrome Enterprise Premium ("CEP"). (ECF No. 1, ¶ 41.) CEP is a secure enterprise Internet browsing solution that provides integrated threat and data protection, offering scalable context-aware access control as software-as-a-service and through web applications, helping to mitigate data exfiltration. *See* https://chromeenterprise.google/solutions/secure-browsing/. (Copy attached as Exhibit 1.) CEP essentially brings together one of the most trusted Google Internet browsers with Google's advanced security capabilities to keep businesses safe. *See* https://chromeenterprise.google/products/chrome-enterprise-premium/. (Copy attached as Exhibit 2). Google's service is available for a monthly fee of $6 per user. (*See id.* at 4). K.Mizra LLC ("K.Mizra") sued Google to collect money damages, in the form of a fully paid up reasonable royalty, for direct infringement of at least claims 19 of U.S. Patent 8,234,705 ("the '705 Patent") and claim 17 of U.S. Patent 9,516,048 ("the '048 Patent"), K.Mizra's zero trust network security patents (collectively "the Asserted Patents") for Google's unauthorized manufacture, sale, and use of CEP. (ECF No. 1).

Google subsequently moved to dismiss that Complaint on two bases ("MTD").[1] First, for allegedly mixing and matching different Google products to arrive at K.Mizra's infringement allegations. (ECF No. 25 at 7-11.) This argument is factually wrong—as below explained, K.Mizra has not mixed and matched different products in presenting its infringement allegations. Second, Google complains that Google cannot legally be liable for direct infringement of the Asserted

[1] Google initially filed its MTD as unopposed (ECF No. 23), later re-filing the current MTD as opposed. (ECF No. 25.) Oddly, both MTDs begin with an Introduction, which is ECF page 5, but is noted as native document page 1. ECF page 6, is native document page 5. K.Mizra is not sure why this page gap exists in the native documents but will herein cite to the ECF page numbers of the opposed MTD for clarity.

Patents. (*Id*. at 11-14.) The argument here is that Google does not provide an allegedly active element of the asserted claims, i.e., the "first host," also sometimes referred to as an "endpoint" computer, the device that seeks to gain access to a protected network. (*Id.*) This argument is legally wrong and, in any case, sounds in claim construction and thus is not procedurally proper to advance at this stage of the proceeding. Accordingly, Google's MTD should be denied. Should the Court disagree, however, K.Mizra requests, per this Court's usual practice, that it be permitted to amend its Complaint after the start of fact discovery so that it might specifically recite additional facts to supplement those found by the Court to be insufficient.

Finally, Google's MTD suggests that K.Mizra seeks pre-suit damages but that K.Mizra failed to plead entitlement thereto in compliance with 35 U.S.C. § 287. (*Id.* at 14-15.) The Complaint includes three paragraphs directed at damages. (ECF No. 1, ¶¶ 58, 78 & B of the Request for Relief.) In none of those paragraphs does K.Mizra seek pre-suit damages.

II. APPLICABLE LEGAL STANDARDS

"A motion to dismiss under rule 12(b)(6) 'is viewed with disfavor and is rarely granted.'" *Collins v. Morgan Stanley Dean Witter*, 224 F.3d 496, 498 (5th Cir. 2000) (quoting *Kaiser Aluminum & Chem. Sales v. Avondale Shipyards*, 677 F.2d 1045, 1050 (5th Cir. 1982)). "The complaint must be liberally construed in favor of the plaintiff, and all" pled facts must be taken as true. *Id.* (quoting *Campbell v. Wells Fargo Bank*, 781 F.2d 440, 442 (5th Cir. 1986)). All reasonably plausible inferences that can be drawn from the pled facts must also be considered and credited when determining whether the defendant could be liable for the misconduct alleged. *Disc Disease Sols. Inc. v. VGH Sols., Inc.*, 888 F.3d 1256, 1260 (Fed. Cir. 2018) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). In a patent case, these facts are that the accused products "meet each and every element of at least one claim." *Id*. "The court's task is to determine whether the

plaintiff has stated a legally cognizable claim that is plausible, not to evaluate the plaintiff's likelihood of success." *Lone Star Fund V (U.S.), L.P. v. Barclays Bank PLC*, 594 F.3d 383, 387 (5th Cir. 2010) (citing *Iqbal*, 556 U.S. at 678). Courts will not dismiss a claim under Rule 12(b)(6) unless the plaintiff "would not be entitled to relief under any set of facts or any possible theory that it could prove consistent with the allegations in the complaint." *Slyce Acquisition, Inc. v. Syte – Visual Conception, Ltd.*, 422 F. Supp. 3d 1191, 1198 (W.D. Tex. 2019) (quoting *Muhammad v. Dallas County Cmty. Supervision & Corr. Dep't*, 479 F.3d 377, 380 (5th Cir. 2007)).

III. ARGUMENT

K.Mizra has presented more than sufficient facts to show it is at least plausible that CEP meets all active limitations of at least one asserted claim of the Asserted Patents. Google's MTD should be denied.

A. Different Products Have *Not* Been Mixed And Matched

Google focuses its mix-and-match argument on claim 19 of the '705 Patent, suggesting three different products, in addition to CEP, were used to demonstrate infringement, with nothing literally or inferentially tying these products together. (ECF No. 25 at 7-11.) Google seems to intentionally misread the Complaint and exalts form over substance.

Complaint Paragraphs 41-58, which incorporate into the body of the Complaint by reference Exhibits 3-12, explain how CEP infringes claim 19 of the '705 Patent. (ECF No. 1, ¶¶ 41-58 and Exs. 3-12.) Google complains that Exhibit 6 is a Google Cloud blog post, Exhibit 10 is a Chrome OS article, and Exhibit 11 is a Google Workspace post, arguing that by reference to these Exhibits means that K.Mizra is improperly mixing-and-matching different products to make its direct infringement allegations. (ECF No. 25 at 7-11.) Not true. As the Complaint explains, CEP is a web application that functions within Google's Cloud environment and ***includes*** features also

found in other Google products. (ECF No. 1, ¶ 48.) In fact, the Complaint specifically here states: "For Example, Google Touts that its Chrome Enterprise product is 'Google Cloud's zero-trust solution that enables an organization's workforce to access web applications securely from anywhere, without the need for VPN and without fear of malware, phishing, and data loss'". (*Id.*) Those features and functions found in both CEP and the other Google products were best explained ***by Google*** in the cited-to Google documents, not in publicly available CEP-centric documents issued by Google. It is for that reason that K.Mizra cited these Google-issued documents concerning other products—they show why CEP infringes. To be clear, though, K.Mizra does not accuse Google Cloud, Chrome OS, or Google Workspace of infringement, only CEP.

1. Element B1—CEP is a Web App that Functions Within Google Cloud

Complaint Paragraph 48 sets the context for what CEP is and the technical context in which it operates, and relevantly reads:

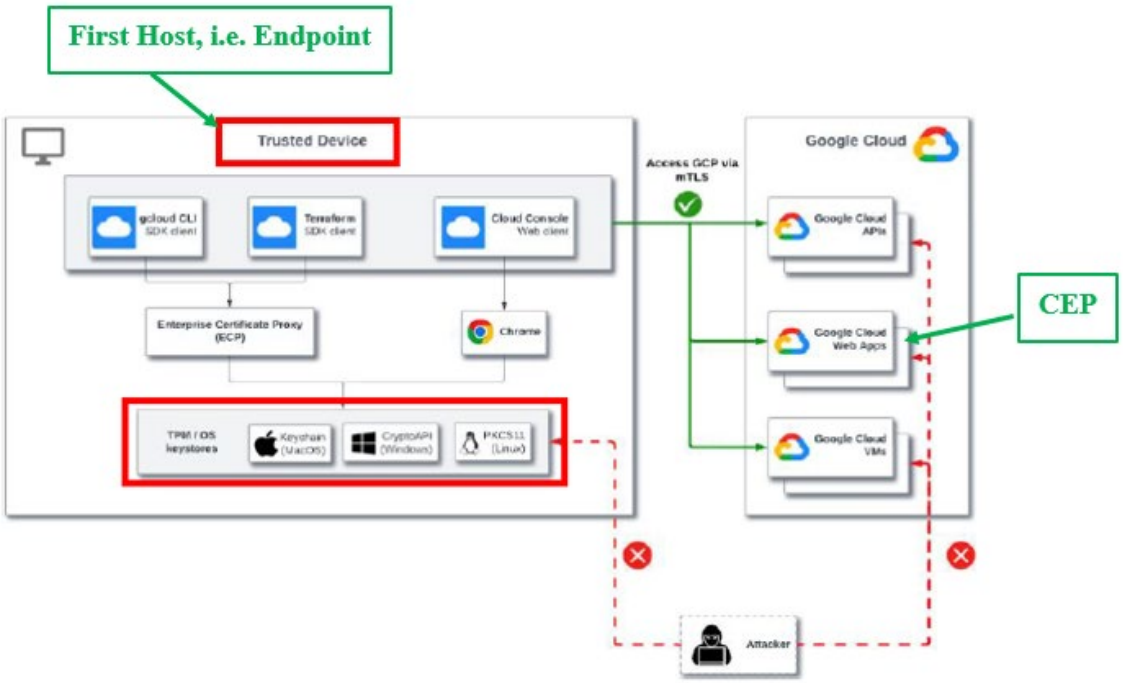
> 48. Regarding the preamble of Claim 19, and to the extent the preamble is determined to be limiting (which it is not), the Accused Instrumentalities provide the features described in the preamble, which recites a "computer program product for protecting a network." For example, Google touts that its Chrome Enterprise product is "Google Cloud's zero-trust solution that enables an organization's workforce to access web applications securely from anywhere, without the need for VPN and without fear of malware, phishing, and data loss":
>
> Chrome Enterprise Premium is Google Cloud's zero-trust solution that enables an organization's workforce to access web applications securely from anywhere, without the need for VPN and without fear of malware, phishing, and data loss.
>
> By using Chrome Enterprise Premium, you can manage access for apps on Google Cloud, other clouds, and on-premises, define and enforce access policies based on user, device, and other contextual factors, and make apps more accessible and responsive through Google's global network.

> *See* Ex. 3, Chrome Enterprise Premium documentation, p. 1 (available at https://cloud.google.com/beyondcorp-enterprise/docs) (last accessed mid Jan. 2025 and incorporated by reference). Additionally, Google's Chrome Enterprise products deliver endpoint (*e.g.*, "host" computer) posture assessments and ensure that endpoints meet security and compliance policies before they are allowed to access a protected network. *See id.* Accordingly, and to the extent the preamble of Claim 19 is deemed limiting, the Accused Zero Trust Network Security Instrumentalities meet the limitation.

(ECF No. 1, ¶ 48.) These factual allegations establish that CEP works within the overarching Google Cloud environment ***and*** functions to "define and enforce access policies based on user, device and other contextual factors" across "Google's global network." These factual allegations, ***which were not credited or even noted by Google in the MTD***, literally (but, if not literally, certainly inferentially) tie CEP to Google Cloud's various "zero trust" access solutions dispersed throughout its various cloud-based products.

Then, Complaint Paragraph 50 relevantly reads:

> 50. Limitation B1 of Claim 19 requires that "detecting [an] insecure condition includes . . . contacting a trusted computing base associated with a trusted platform module within the first host." The Accused Zero Trust Network Security Instrumentalities meet these requirements through, for example, the Google's Chrome Enterprise product which uses "strong key protection" such as "secure cryptographic storage such as TPMs and OS keystores." *See* Ex. 6, How To Prevent Account Takeovers With New Certificate-Based Access, p. 1 (available at https://cloud.google.com/blog/products/identity-security/how-to-prevent-account-takeovers-with-new-certificate-based-access) (last accessed mid Jan. 2025 and incorporated by reference).



See id. at 2. The Accused Zero Trust Network Security Instrumentalities obtain information from the host computer through digitally-signed certificates to determine whether the host computer is secure and can be trusted to access the protected network:

(*Id.*, ¶ 50.)

Contrary to Google's argument (ECF No. 25 at 8-9), these allegations establish that CEP is designed to and does "contact" a "trusted computing base" ("TCB") "associated with a trusted platform module" ("TPM") located within a "first host" to "detect" whether an insecure condition exists on the "first host." The above Google figure, now annotated in green above for ease of reference, shows that Web Apps, like the CEP Web App, sit within the Google Cloud and can communicate with a Trusted Device, i.e. a "first host," that uses a TPM and thus a TCB. That request from CEP to the TCB located within the "first host" is made "via mTls," a secure communication protocol/technology that is further explained in Complaint Paragraph 51. (ECF No. 1, ¶ 51.) Google's complaints concerning the use of a Google Cloud blog and Google-created figure to explain how CEP functions within Google's Cloud ecosystem are just wrong. It appears

that Google is really raising a claim construction dispute over the meaning of the term "contact" in claim 19. But this kind of dispute is best left to the claim construction process and is inappropriate for a motion to dismiss. *See Unification Techs. LLC v. Dell Techs., Inc.*, No. 6:20-CV-00499-ADA, 2021 WL 1343188, at 3 (W.D. Tex. Jan. 28, 2021) (denying a Motion to Dismiss because "a 12(b)(6) motion is not the appropriate procedure for identifying inconsistent direct infringement contentions. Those are premature assertions that are best addressed in claim construction or non-infringement positions."); *Kirsch Rsch. & Dev., LLC v. BlueLinx Corp.*, No. 6-20-CV-00316-ADA, 2021 WL 12300174, at 4 (W.D. Tex. July 19, 2021) (denying a Motion to dismiss because "to engage in pre-Markman claim construction and resolve that construction [] is premature."); *Repairify, Inc. v. Keystone Automotive Indus., Inc.*, 610 F. Supp. 3d 897, 903 (W.D. Tex. 2022) (the Court would not entertain a Motion to Dismiss on claim construction grounds).

Finally, Google's reliance on this Court's decision in *Grecia* (ECF No. 25 at 9) is misplaced. In that case, the plaintiff

> resorted to parroting claim language when pressed at a hearing before this Court to identify an accused instrumentality of the encrypted digital media, insisting only that Facebook Pay's encrypted digital media is the encrypted digital media. The mere recitation of claim language, however, is insufficient to assert a claim, even on a motion to dismiss. Thus, Grecia's contentions cannot lead to a reasonable inference that Facebook Pay *brands* the metadata of the encrypted digital media. . . . In this Court's judgment, Grecia's allegation without explanation is threadbare at best.

Grecia Estate Holdings LLC v. Meta Platforms, Inc., 605 F. Supp. 3d 905, 916-17 (W.D. Tex. 2022). Unlike in *Grecia*, K.Mizra here provided a Google-produced document that shows exactly how its accused system works, which is more than sufficient under modern pleading standards.[2]

[2] Perhaps K.Mizra should have annotated the figure in the Complaint as it does above. But to be fair, Google should know how its products function and the above drawing should easily have provided Google with notice of what it is here being accused, and that is all that is required. *Disc*

2. Element C—Verified Access is a Feature of Both CEP and Chrome OS

K.Mizra explains in Paragraph 49 of its Complaint that CEP includes "endpoint verification." An "endpoint" is a "first host" and "verification" objectively means in the context of network security systems that CEP checks with the "first host" to confirm that it meets all established security and compliance policies before it is allowed to connect to the protected network. (ECF No. 1, ¶ 49.) In this Complaint paragraph, K.Mizra also incorporates by reference the entirety of two Google-produced documents (unchallenged by Google in its MTD), Exhibits 4 and 5, which explain various features/functionality of CEP, including "endpoint verification." Important to Google's argument here, Exhibit 5 provides the following explanation of some CEP functions/features as compared to Google Cloud:

Chrome Enterprise Premium compared with Google Cloud

Chrome Enterprise Premium provides enterprise security features in addition to the basic protections, focused on protecting applications with authentication and authorization, that are baseline features of Google Cloud. Chrome Enterprise Premium extends those protections to applications and data running everywhere, with end-user protections and rich access policy protections.

The following table shows the differences between the baseline features available to Google Cloud customers and what is available with Chrome Enterprise Premium:

Applications and Resources Access	GCP Baseline	BeyondCorp Enterprise Essentials	BeyondCorp Enterprise
Access control to web applications on Google Cloud Platform	✓		✓
Access control to SSH, RDP and TCP ports for VMs on GCP	✓		✓
Access control to Google Cloud Platform APIs	✓		✓
Access control to Google Cloud console	✓		✓
Access control to web applications on GCP internal load balancing	✓		✓
Access control to web applications on customer premises			✓
Access control to thick client / client-server applications			✓
Access control to web applications on AWS and Azure			✓
Access control to SAML-based applications (login time)		✓	✓
Access control to Google Workspace Admin Console		✓	✓
Access Policies and Advanced Settings	**GCP Baseline**	**BeyondCorp Enterprise Essentials**	**BeyondCorp Enterprise**

Disease Sols., 888 F.3d at 1260 (quoting *Iqbal*, 556 U.S. at 678) ("'Specific facts are not necessary; the statement need only give the defendant fair notice of what the . . . claim is and the ground upon which it rests.'" *Id.* (quoting *Erickson v. Pardus*, 551 U.S. 89, 93 (2007)) (alteration in original) (internal quotation marks omitted) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

(ECF No. 1, Ex. 5 at 4.) What this Google document relevantly conveys is that Google Cloud (i.e., basic Chrome) and CEP (i.e., Chrome Enterprise Premium, formerly called BeyondCorp Enterprise) both provide Access Control to Google Platform APIs (*see* yellow highlighted box above). In Paragraph 52 of the Complaint, K.Mizra alleges that Verified Access is a particular type of Google API, with the logical inference of that factual allegation being that CEP makes calls to the Verified Access API and by doing so meets limitation C of claim 19 of the '705 Patent. K.Mizra's reliance on a Google Cloud document to explain how Access Control and Verified Access works in both CEP and Google Cloud, more generally, is not an allegation of infringement against Google Cloud, but rather an explanation of how CEP infringes Claim 19 by calling Google's Verified Access API and thus determining whether the "first host" is "clean" or "infested."

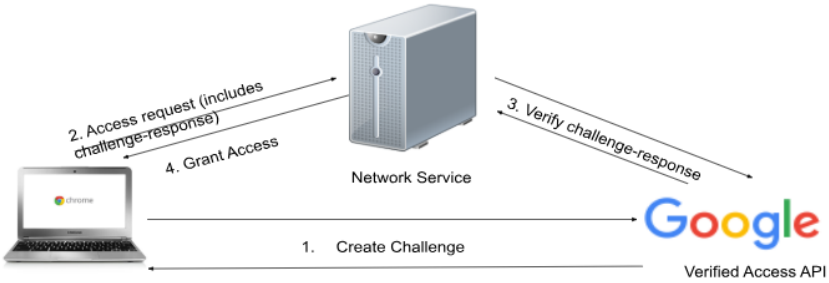
K.Mizra could have cited to https://developers.google.com/chrome/verified-access/overview (copy attached hereto as Exhibit 3) to make the same point, a Google document updated October 16, 2024 and showing how the Verified Access API is called by Chrome and thus also CEP:

About Chrome Verified Access

Your network service can use the Verified Access feature in the Google Admin console to communicate with both the client Chrome device and the Verified Access API. Doing so gains information about the policy compliance and (optionally) the identity of the client device from Google. To that end, a Chrome extension must be running on the device that interacts with the enterprise.platformKeys extension API, and the network service needs to talk to the Verified Access API.

How Chrome Verified Access Works

Here's the suggested implementation:



Suggested implementation.

1. The Chrome extension contacts the Verified Access API to create a challenge.
2. The Chrome extension calls the enterprise.platformKeys API to generate a challenge-response and sends the access request to the network service, including the challenge-response in the request.
3. The network service contacts the Verified Access API to verify the challenge-response.
4. In case of successful verification, the network service grants access to the device.

(Ex. 3 at 2.) But the fact remains that CEP calls Google's Verified Access API, and by doing so determines whether the "first host" is "clean" or "infested." If it is the latter, the "first host" is not allowed to join the secure network. These functions satisfy the requirements of limitation C of claim 19, at least as they should be properly understood by a skilled artisan reviewing the intrinsic record of the Asserted Patents. Thus, contrary to Google's argument (ECF No. 25 at 9-10), the Complaint ties the functions of CEP to calling Verified Access API and explains that API's function meets the requirements of limitation C of Claim 19. K.Mizra's allegations are clearly sufficient to put Google on notice of its theory of infringement, which is all that is required. *See Twombly*, 550 U.S. at 556. ("Specific facts are not necessary"; the statement need only 'give the defendant fair notice of what the . . . claim is and the ground upon which it rests.'")

Finally, Google's reliance on *Ortiz & Assocs.*, another decision issued by this Court (*id.* at 10), is again misplaced. In that case, the plaintiff filed both a complaint and then an amended complaint, with the Court finding:

> In Ortiz's Amended Complaint, Ortiz provided a chart that displays the claim language on one side and the accused product details on the other, accompanied by a brief description. ECF No. 16. However, ***Ortiz fails to identify an essential element in the claim chart***—the server. Id. Ortiz's Amended Complaint lacks any explanation of the existence of a server despite the claim requiring "memory in said server accessibly by said [data rendering device]." ECF No. 16-1 at cl. 1. Without so much as identifying the existence of a server, Ortiz fails to plausibly suggest that the accused product meets each limitation of the asserted claim.

Ortiz & Assocs. Consulting, LLC v. Ricoh USA, Inc., No. 6:21-CV-01178-ADA, 2023 WL 2904583, at *4 (W.D. Tex. Apr. 11, 2023). Here, K.Mizra has specifically pointed to the evidence upon which it relies to satisfy limitation C of claim 19 of the '705 Patent—this is not a case where K.Mizra just failed to address a limitation ***at all***. Google knows how CEP functions and the Complaint explains how it meets all the claims limitations, and that is all that is required. *Disc Disease Sols.*, 888 F.3d at 1260 (quoting *Iqbal*, 556 U.S. at 678) ("'Specific facts are not necessary; the statement need only give the defendant fair notice of what the . . . claim is and the ground upon which it rests.'" *Id.* (quoting *Erickson*, 551 U.S. at 93) (alteration in original) (internal quotation marks omitted) (quoting *Twombly*, 550 U.S. at 555).

3. Element D—Context-Aware Access is a Feature of Both CEP and Workspace

K.Mizra explains in Paragraph 53 of its Complaint that CEP meets limitation D of claim 19 of the '705 Patent and that it is met by calling to a Web App called Context-Aware Access (ECF No. 1, ¶ 53):

53. Limitation D requires that "when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network." The Accused Zero Trust Network Security Instrumentalities further meet these requirements by quarantining noncompliant, *i.e.*, unclean, endpoint devices attempting to connect to the protected network:

> Using Context-Aware Access, admins can set up different access levels based on a user's identity and the context of the request (location, device security status, IP address). This can help provide granular access controls without the need for a VPN, and give users access to Google Workspace resources based on organizational policies. Insights and recommendations help admins improve the cybersecurity posture of their organization by proactively identifying areas that need attention, significantly reducing the need for admins to identify these risks themselves. For example, if we detect devices with outdated operating system versions accessing corporate Workspace data, we can surface this as an Insight & pair it with a recommendation to block such devices from accessing Workspace data with a few clicks.

See Ex. 10, Context Aware Access Insights and Recommendations Are Now Generally Available, p. 3 (available at https://workspaceupdates.googleblog.com/2024/10/context-aware-access-insights-and-recommendations.html) (last accessed mid Jan. 2025 and incorporated by reference).

> Using context-aware access, you now have the option to automatically block access to Google Workspace data from compromised Android and iOS devices. A device may be counted as compromised if certain unusual events are detected, including devices that are jailbroken, bypassing of security controls, modification of restricted settings, and more.

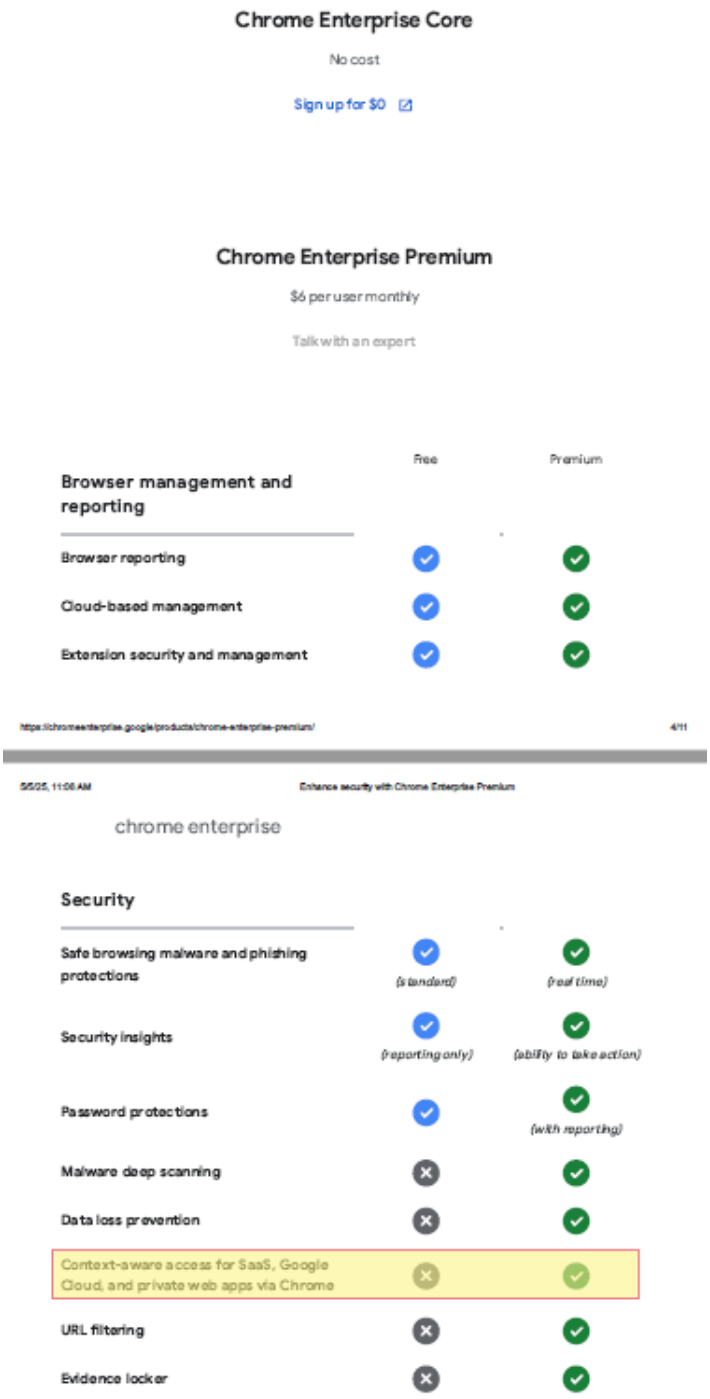
See Ex. 11, Block Compromised Mobile Devices Using Context-Aware Access, p. 2 (available at https://workspaceupdates.googleblog.com/2024/05/block-compromised-mobile-devices-using-context-aware--access.html) (last accessed mid Jan. 2025 and incorporated by reference). Accordingly, the Accused Zero Trust Network Security Instrumentalities meet limitation D of Claim 19.

(ECF No. 1, ¶ 53.)

Context-Aware Access is another feature/function of the CEP product that allows for and facilitates quarantining of endpoints, i.e., a "first hosts." Google's specific argument here is that

Complaint Paragraph 53 does not textually plead that Context-Aware Access is a Web App that can both be called by Google's Workspace and CEP products. (ECF No. 25 at 11.) Complaint Paragraph 53 plausibly, through an objectively reasonable inference, advised Google that CEP calls Context-Aware Access and that functionality satisfies limitation D of claim 19 of the '705 Patent. *See Disc Disease Sols.,* 888 F.3d at 1260.

If the Court disagrees that K.Mizra properly pled CEP included limitation D of claim 19 of the '705 Patent, there is no question but that K.Mizra could amend to add sufficient allegation on this element. For instance *see* Exhibit 2, which indicates that Context-Aware Access is a security feature of CEP:



4. The Court's *CDT* Decision Confirms that Denial of Google's MTD is Warranted

Finally, and contrary to Google's position that *CTD Networks, LLC v. Google, LLC*, 688 F. Supp. 3d 490, 499 (W.D. Tex. 2023) supports dismissal, a review of this Court's analysis from that

case confirms that **denial** of Google's MTD is here warranted. In the *CTD Networks* case, Google alleged, as it does here, that plaintiff mixed and matched various Google products to arrive at infringement. In there agreeing with Google, this Court held:

> ***At a minimum, Plaintiff would need allegations to support a theory that the various products worked together in concert to perform the claims as written, which CTD's allegations do not establish.*** At most, CTD alleges only that the products are part of a "suite" sold on Google's website. The fact that the products may be sold or marketed together is irrelevant where, as here, each "asserted patent claims require that a single 'agent' perform each of the claimed functions . . . ." ECF No. 44 at 11. CTD merely points out "disparate aspects of entirely different products as allegedly performing each claimed functionality." *Id.*

Id. at 500. Unlike plaintiff in *CTD* after filing three complaints, K.Mizra did exactly as this Court counseled, pleading allegations in its original Complaint that the various features and functions incorporated into CEP are designed to and do work together. (ECF No. 1, ¶ 48.)

B. The Asserted Claims Do Not Require Third Party Actors

Google argues that it can only infringe asserted claims 19 or 17 of the '705 and '048 Patents, respectively, under a non-pled contributory or induced infringement theory, as it does not supply the "first host" found in the asserted claims. (ECF No. 25 at 11-14.) Google's argument is that "first host," i.e., the endpoint computer, such as a laptop, smartphone, tablet, is an active element of the claims that is not provided by Google, so it cannot ***directly infringe*** any claims of either patent. However, the claim language dictates what is and is not an active element. The "first host" is not an active element. Rather, it is simply a component of the "environment" in which the active claim elements must function. Thus, Google's failure to supply the "first host" is irrelevant to holding Google liable for direct infringement of these claims.

Recently, the Federal Circuit explained "environmental" claiming and the role it plays in determining direct infringement. *INVT SPE LLC v. Int'l Trade Comm'n*, 46 F.4th 1361 (Fed. Cir. 2022). As explained in *INVT:*

> [t]he base station is part of "the environment" in which the [actively claimed] user device must function. *Advanced Software Design Corp. v. Fiserv, Inc.,* 641 F.3d 1368, 1374 (Fed. Cir. 2011). The claims have specific requirements for the data signal that the user device's receiving section and data obtaining section handle and process when the device is activated and put into operation. . . . To understand whether a user device can ever receive a data signal with the particularized characteristics set forth in the claim, it is necessary to know whether the base station (i.e., the communicating party) is capable of transmitting that particular type of data signal to the user device. ***Therefore, although the recited base station is not "a limitation on the claimed invention itself,"*** *Nazomi Communs., Inc. v. Nokia Corp.,* 739 F.3d 1339, 1345 (Fed. Cir. 2014*)*, ***in the sense that an infringer would not need to, for instance, use, make, or sell the base station***, the base station's operation affects whether the claims are met, *see, e.g.*, *Advanced Software Design,* 641 F.3d at 1373-74.
>
> In *Advanced Software*, the claimed invention was for validating a check, to prevent check fraud, and involved either decrypting or encrypting information on the check. The preamble of the claim set out that the check included "selection information [that] is encrypted" to generate a control code and a "control code [which] is printed on the [check]." We held that these steps in the preamble "define[d] the financial instrument that the claimed system validates" as opposed to setting forth steps that would have to be performed by the accused infringer. *Advanced Software*, 641 F.3d at 1373-74 & 1374 n.1. Nevertheless, the accused infringer would infringe "only by validating checks that [had] been encrypted and printed in accordance with steps described in the preamble." *Id*. at 1374.
>
> Like in *Advanced Software*, the claimed device of the [INVT] patent operates in an environment that involves actions of another device (the communicating party, i.e., the base station). The claimed device's capability of performing the recited functions depends on being supplied a certain modulated and encoded signal, which, in turn, requires the supplier (the communicating party) to actually supply that signal. Because the communicating party (base station) generates the necessary environment, its operations must be known to determine whether the accused device infringes, i.e., is capable of performing the claimed functions.

Id. at 1375 (emphasis added); *see also Uniloc USA, Inc. v. Microsoft Corp*., 632 F.3d 1292, 1308-09 (Fed. Cir. 2011) (holding that claimed "station forming part of a registration system . . . including local licensee unique ID generating means," only "define[d] the environment in which that [remote] registration station must function.").

Claim 19 of the asserted '705 Patent recites a "computer program product for protecting a network . . ." that can perform the following active functions:

Receiving a service request from a first host;

Contacting a trusted computing base (TCB) associated with a trusted platform module (TPM) located within the first host;

Receiving a response from the TCB;

Determining from that response whether the first host is infested or clean;

Quarantining, if infestation is detected, the first host; and

Permitting the first host to communicate with a remediation host.[3]

CEP is a computer program product that protects computer networks and performs each active recited function of the claims, i.e., the bolded terms. The rest of the claim, specifically including the "first host," is environment within which the active verbs of the claim must operate. To be sure, K.Mizra will need to present evidence of how CEP interacts with a "first host" and its various

[3] Claim 19, with the active verbs highlighted, is here provided for ease of reference:

19. A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising computer instructions for:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network, wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request, and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and

permitting the first host to communicate with the remediation host.

components. That said, K.Mizra does not need to establish that Google supplies the "first host" for it to prove that Google directly infringes the asserted claims.

If Google disagrees with K.Mizra's literal reading of the relevant claim language, it can make its argument during the claim construction phase of this action, but that is not an appropriate issue to raise on a motion to dismiss. *See e.g., Fintiv, Inc. v. PayPal Holdings, Inc.*, No. 6:22-CV-288-ADA, 2022 WL 22870185, at *4 (W.D. Tex. Dec. 19, 2022) ("Because the Court has not construed the claims and because the parties have not engaged in discovery, it is premature for the Court to hold that the claims in the Asserted Patents require acts of third parties that [Google] is incapable of performing. *See BillJCo, LLC v. Cisco Sys., Inc.*, No. 2:21-CV-181, 2021 WL 6618529, at *4 (E.D. Tex. Nov. 30, 2021) ('At the 12(b)(6) stage, the parties have neither completed claim construction discovery nor briefed claim construction related issues. The Court therefore declines to determine at this juncture whether asserted method claims require multiple steps or which actors must perform those steps.')").

IV. CONCLUSION

The Court should deny Google's MTD in its entirety. However, should the Court grant all or some of the MTD, given the difficulty in alleging more specific details without the benefit of fact discovery and in accordance with the Court's usual practice, K.Mizra requests that the Court permit it to amend its Complaint after the start of fact discovery to specifically recite any claim elements and/or underlying facts that would supplement the currently-pled facts found to be insufficient by the Court.

Dated: May 12, 2025

Respectfully submitted,

By: /s/ Robert R. Brunelli

Michael C. Smith
Texas Bar No. 18650410
michael.smith@solidcounsel.com

Scheef & Stone, LLP
113 E. Austin Street
Marshall, TX 75670
(903) 938-8900

Robert R. Brunelli (Admitted *pro hac vice*)
CO State Bar No. 20070
rbrunelli@sheridanross.com
Bart A. Starr (Admitted *pro hac vice*)
CO State Bar No. 50446
bstarr@sheridanross.com
Brian S. Boerman (Admitted *pro hac vice*)
CO State Bar No. 50834
bboerman@sheridanross.com
Gene Volchenko (Admitted *pro hac vice*)
IL State Bar No. 6342818
gvolchenko@sheridanross.com
SHERIDAN ROSS P.C.
1560 Broadway, Suite 1200
Denver, CO 80202
Telephone: 303-863-9700
litigation@sheridanross.com

Of Counsel:
Claire A. Henry
Texas Bar No. 24053063
Miller Fair Henry PLLC
1507 Bill Owens Parkway
Longview, TX 75604
Telephone: (903) 757-6400
claire@millerfairhenry.com

Attorneys for Plaintiff K.Mizra LLC

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the above and foregoing document has been served on May 12, 2025, to all counsel of record who are deemed to have consented to electronic service via the Court's CM/ECF system.

/s/ Lori R. Brown
Lori R. Brown
lbrown@sheridanross.com
SHERIDAN ROSS P.C.
1560 Broadway, Suite 1200
Denver, CO 80202
Telephone: 303-863-9700
Facsimile: 303-863-0223